受領書

平成１１年　７月１９日
特　許　庁　長　官

識別番号　　１００００７８８６８
氏名（名称）　　河野　登夫　　殿
提出日　　平成１１年　７月１９日

以下の書類を受領しました。

項番	書類名	整理番号	受付番号	出願番号通知（事件の表示）
1	出願審査請求	092242S	59900695140	特願平 4-209082
2	出願審査請求	092241S	59900695141	特願平 4-209083
3	特許願	20298	59900695142	特願平11-205379
4	特許願	20400	59900695145	特願平11-205380
5	特許願	20399	59900695146	特願平11-205381
6	特許願	100939	59900695148	特願平11-205382
7	特許願	20318	59900695150	特願平11-205383

以　上

20399
3000208860

提出日　平成１１年　７月１９日
整理番号＝２０３９９　　頁:　1/　2

11－205381

【書類名】　特許願
【整理番号】　２０３９９
【提出日】　平成１１年　７月１９日
【あて先】　特許庁長官殿
【国際特許分類】　Ｈ０４Ｌ　９／１４
Ｈ０４Ｌ　９／３０
Ｇ０９Ｃ　１／００
【発明の名称】　暗号化方法，暗号通信方法及び暗号文作成装置
【請求項の数】　３
【発明者】
【住所又は居所】　大阪府箕面市粟生外院４丁目１５番３号
【氏名】　笠原　正雄
【発明者】
【住所又は居所】　京都府京都市伏見区竹田向代町１３６番地　村田機械株式会社　本社工場内
【氏名】　村上　恭通
【特許出願人】
【識別番号】　０００００６２９７
【氏名又は名称】　村田機械株式会社
【代表者】　村田　純一
【特許出願人】
【識別番号】　５９７００８６３６
【氏名又は名称】　笠原　正雄
【代理人】
【識別番号】　１００７８８６８
【弁理士】
【氏名又は名称】　河野　登夫
【電話番号】　０６－６９４４－４１４１
【手数料の表示】

【予納台帳番号】　００１８８９

【納付金額】　２１０００

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　９８０５２８３

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　暗号化方法，暗号通信方法及び暗号文作成装置

【特許請求の範囲】

【請求項１】　暗号化すべき平文を分割した平文ベクトルと公開鍵ベクトルとを用いて暗号文を作成する暗号化方法において、前記平文ベクトルの一部と前記公開鍵ベクトルの一部とによる積和項を複数設定し、設定した複数の積和項を積及び／または和の形式で結合することにより前記暗号文を作成することを特徴とする暗号化方法。

【請求項２】　一方のエンティティ側で平文を分割した平文ベクトルと公開鍵ベクトルとを用いて暗号文を作成して他方のエンティティ側へ伝送し、伝送された暗号文を該他方のエンティティ側で元の平文に復号することにより、エンティティ間で情報の通信を行う暗号通信方法において、前記平文ベクトルの一部と前記公開鍵ベクトルの一部とによる積和項を複数設定し、設定した複数の積和項を積及び／または和の形式で結合することにより前記暗号文を作成し、作成した暗号文を前記他方のエンティティへ伝送することを特徴とする暗号通信方法。

【請求項３】　平文から暗号文を作成する装置において、前記平文を分割する手段と、分割した複数の平文ベクトルの一部と公開鍵ベクトルの一部とによる積和項を複数設定する手段と、設定した複数の積和項を積及び／または和の形式で結合することにより前記暗号文を作成する手段とを備えることを特徴とする暗号文作成装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、平文を積和型の暗号文に変換するための暗号化方法、この暗号化方法を利用した暗号通信方法、及び、その暗号文を作成する暗号文作成装置に関する。

【０００２】

【従来の技術】

高度情報化社会と呼ばれる現代社会では、コンピュータネットワークを基盤と

して、ビジネス上の重要な文書・画像情報が電子的な情報という形で伝送通信されて処理される。このような電子情報は、容易に複写が可能である、複写物とオリジナルとの区別が困難であるという性質があり、情報保全の問題が重要視されている。特に、「コンピュータリソースの共有」，「マルチアクセス」，「広域化」の各要素を満たすコンピュータネットワークの実現が高度情報化社会の確立に不可欠であるが、これは当事者間の情報保全の問題とは矛盾する要素を含んでいる。このような矛盾を解消するための有効な手法として、人類の過去の歴史上主として軍事，外交面で用いられてきた暗号技術が注目されている。

【０００３】

暗号とは、情報の意味が当事者以外には理解できないように情報を交換することである。暗号において、誰でも理解できる元の文（平文）を第三者には意味がわからない文（暗号文）に変換することが暗号化であり、また、暗号文を平文に戻すことが復号であり、この暗号化と復号との全過程をまとめて暗号系と呼ぶ。暗号化の過程及び復号の過程には、それぞれ暗号化鍵及び復号鍵と呼ばれる秘密の情報が用いられる。復号時には秘密の復号鍵が必要であるので、この復号鍵を知っている者のみが暗号文を復号でき、暗号化によって情報の秘密性が維持され得る。

【０００４】

暗号化方式は、大別すると共通鍵暗号系と公開鍵暗号系との二つに分類できる。共通鍵暗号系では、暗号化鍵と復号鍵とが等しく、送信者と受信者とが同じ共通鍵を持つことによって暗号通信を行う。送信者が平文を秘密の共通鍵に基づいて暗号化して受信者に送り、受信者はこの共通鍵を用いて暗号文を元に平文に復号する。

【０００５】

これに対して公開鍵暗号系では、暗号化鍵と復号鍵とが異なっており、公開されている受信者の公開鍵で送信者が平文を暗号化し、受信者が自身の秘密鍵でその暗号文を復号することによって暗号通信を行う。公開鍵は暗号化のための鍵、秘密鍵は公開鍵によって変換された暗号文を復号するための鍵であり、公開鍵によって変換された暗号文は秘密鍵でのみ復号することができる。

【０００６】

【発明が解決しようとする課題】

公開鍵暗号系の１つの方式として、積和型暗号方式が知られている。これは、送信者である一方のエンティティ側で平文をＫ分割した平文ベクトルｍ＝（m_1，m_2，・・・，m_K）と公開鍵である基数ベクトルｃ＝（c_1，c_2，・・・，c_K）とを用いて、暗号文Ｃ＝$m_1 c_1 + m_2 c_2 + \cdots + m_K c_K$を作成し、受信者である他方のエンティティ側でその暗号文Ｃを秘密鍵を用いて平文ベクトルｍに復号して元の平文を得る暗号化形式である。

【０００７】

このような整数環上の演算を利用した積和型暗号に関して、新規な方式及び攻撃法が次々に提案されているが、特に、多くの情報を短時間で処理できるように高速復号可能な暗号化・復号の手法の開発が望まれている。そこで、本発明者等は、多進法を用いることにより、高速な復号処理を可能とした積和型暗号における暗号化方法及び復号方法を提案している（特願平10－262036号，特願平10－262037号）。

【０００８】

この暗号化方法は、基数ベクトルｃの成分c_i（ｉ＝１，２，・・・，Ｋ）を、整数b_iを用いて$c_i = b_1 b_2 \cdots b_i$に設定する、或いは、整数b_i，乱数v_iを用いて$c_i = v_i b_1 b_2 \cdots b_i$に設定する（特願平10－262036号）、または、基数ベクトルｃの成分c_i（ｉ＝１，２，・・・，Ｋ）を、互いに素なＫ個の整数d_iを用いて$c_i = d / d_i$（但し、$d = d_1 d_2 \cdots d_K$）に設定する、或いは、互いに素なＫ個の整数d_i，乱数v_iを用いて$c_i = (d / d_i) v_i$に設定する（特願平10－262037号）ことを特徴としている。このようにして、平文を多進法を用いて表現するようにしたので、高速な復号を行うことができる。

【０００９】

元来、このような積和型暗号化方法は、公開されている基数ベクトルｃの各成分から平文ｍの各成分を解読する数学的なＬＬＬ（Lenstra-Lenstra-Lovasz）法による攻撃を受け易いという特徴を持っており、このＬＬＬ法に対して強い積和

型暗号化方法の開発が望まれている。

【００１０】

本発明は斯かる事情に鑑みてなされたものであり、ＬＬＬ法による攻撃に対して強く、安全性を向上できる暗号化方法、この暗号化方法を利用した暗号通信方法、及び、その暗号文を作成する暗号文作成装置を提供することを目的とする。

【００１１】

【課題を解決するための手段】

請求項１に係る暗号化方法は、暗号化すべき平文を分割した平文ベクトルと公開鍵ベクトルとを用いて暗号文を作成する暗号化方法において、前記平文ベクトルの一部と前記公開鍵ベクトルの一部とによる積和項を複数設定し、設定した複数の積和項を積及び／または和の形式で結合することにより前記暗号文を作成することを特徴とする。

【００１２】

請求項２に係る暗号通信方法は、一方のエンティティ側で平文を分割した平文ベクトルと公開鍵ベクトルとを用いて暗号文を作成して他方のエンティティ側へ伝送し、伝送された暗号文を該他方のエンティティ側で元の平文に復号することにより、エンティティ間で情報の通信を行う暗号通信方法において、前記平文ベクトルの一部と前記公開鍵ベクトルの一部とによる積和項を複数設定し、設定した複数の積和項を積及び／または和の形式で結合することにより前記暗号文を作成し、作成した暗号文を前記他方のエンティティへ伝送することを特徴とする。

【００１３】

請求項３に係る暗号文作成装置は、平文から暗号文を作成する装置において、前記平文を分割する手段と、分割した複数の平文ベクトルの一部と公開鍵ベクトルの一部とによる積和項を複数設定する手段と、設定した複数の積和項を積及び／または和の形式で結合することにより前記暗号文を作成する手段とを備えることを特徴とする。

【００１４】

本発明では、平文ベクトルの一部と公開鍵ベクトルの一部とによる複数の積和項を、更に、積及び／または和の形式で結合することにより暗号文を作成する。

即ち、平文ベクトルｍ，公開鍵ベクトルｃに対して、下記（１）のようにして暗号文Ｃを作成する。

【００１５】

【数１】

$$C=\sum_{i}\prod_{j}\sum\cdots\prod\sum\cdots\sum_{p}m_{ij\cdots p}c_{ij\cdots p}\quad\cdots(1)$$

【００１６】

例えば、平文を８分割した平文ベクトルｍ＝（m_1，m_2，・・・，m_8）と公開鍵ベクトルｃ＝（c_1，c_2，・・・，c_8）とを用いて、下記（２），（３）のようにして、暗号文Ｃを作成する。

$$C=(m_1c_1+m_2c_2+m_3c_3)\times(m_4c_4+m_5c_5)\times(m_6c_6+m_7c_7+m_8c_8)\quad\cdots(2)$$

$$C=(m_1c_1+m_2c_2)\times(m_3c_3+m_4c_4)+(m_5c_5+m_6c_6)\times(m_7c_7+m_8c_8)\quad\cdots(3)$$

【００１７】

上記（２）では、平文ベクトルｍの一部及び公開鍵ベクトルｃの一部を用いた３種類の積和項を更に乗算した形式にて、暗号文Ｃを作成している。よって、従来のものを積和型の暗号文とした場合、この（２）は、積和積型の暗号文と言える。一方、上記（３）では、第１及び第２の積和項を乗算すると共に第３及び第４の積和項を乗算し、夫々の乗算結果を加算した形式にて、暗号文Ｃを作成している。よって、この（３）は、積和積和型の暗号文と言える。

【００１８】

このように、複数の積和項を乗算及び／または加算にて結合した形式の暗号文を作成しており、ＬＬＬ法で攻撃された場合にも、複数の積和項がどのように組み合わさって結合されているかが不明であるので、ＬＬＬ法による攻撃に強い暗号文を作成できる。

【００１９】

なお、このような形式で示される暗号文は、特願平10－262036号に提案したｂ

$_i$進数復号法，特願平10－262037号に提案した中国人の剰余定理を用いて高速復号することができる。

【００２０】

【発明の実施の形態】

以下、本発明の実施の形態について具体的に説明する。

図１は、本発明による暗号化方法・復号方法をエンティティａ，ｂ間の情報通信に利用した状態を示す模式図である。図１の例では、一方のエンティティａ側で、平文ｘを暗号文Ｃに暗号化し、通信路１を介してその暗号文Ｃを他方のエンティティｂへ送信し、エンティティｂ側で、その暗号文Ｃを元の平文ｘに復号する場合を示している。

【００２１】

送信側であるエンティティａには、平文ｘを平文ベクトルｍに分割する平文分割器２と、この平文ベクトルｍの一部と公開鍵ベクトルｃの一部とを用いて複数の積和項を設定する積和項設定器３と、設定された複数の積和項を積及び／または和の形式で結合して暗号文Ｃを作成する暗号化器４とが備えられている。また、受信側であるエンティティｂには、送られてきた暗号文Ｃを元の平文ｘに復号する復号器５が備えられている。

【００２２】

本発明では、上記（１）のように、乗算及び／または加算の演算を自由に用いて複数の積和項を結合させて暗号文Ｃを作成する。以下では、本発明の最も簡単な形式である積和積型の暗号文（上記（２）のように、複数の積和項を乗算により結合させた形式の暗号文）を例にして説明する。

【００２３】

平文ｘを分割した平文ベクトルｍの成分（メッセージ）の大きさm_iは下記（４）を満たし、基数b_iは下記（５）を満たす素数とする。

$$m_i < 2^e \qquad \cdots (4)$$

【００２４】

【数２】

$$b_i = 2^e + \delta_i \quad (1 \ll \delta_i \ll 2^e) \quad \cdots(5)$$

【００２５】

秘密鍵と公開鍵とを以下のように準備する。

・秘密鍵：$\{b_i\}$，P，w

・公開鍵：$\{c_i\}$

【００２６】

乱数wを用いて、公開鍵$\{c_i\}$を下記（６）のように求める。

$$c_i \equiv w b_1 b_2 \cdots b_i \pmod{P} \quad \cdots(6)$$

【００２７】

暗号文Cは、メッセージ$\{m_i\}$の一部と公開鍵$\{c_i\}$の一部とによる積和演算結果を更に乗算した形で与えられる。暗号文Cは、下記（７）のように表される。

$$C \equiv C_1 \cdot C_2 \cdot C_3 \cdots C_I \pmod{P} \quad \cdots(7)$$

【００２８】

暗号文Cは、実質的にはＩ分割されており、これらのＩ個の分割暗号文の乗算形式で構成されている。各分割暗号文は、平文の分割ベクトルの一部の成分と公開鍵ベクトルの一部の成分とによる積和項で構成されている。

【００２９】

以下のようにして復号処理が行われる。暗号文Cに対して、中間復号文M_Iを下記（８）のようにして求める。

$$M_I \equiv S_1 \cdot S_2 \cdot S_3 \cdots S_I \pmod{P} \quad \cdots(8)$$

但し、S_iは、下記（９）で表され、$P^{(i)}$は、一般に下記（10）の条件を満たす大きな素数であり、Pのみを公開する。なお、Hは分割暗号文の中の暗号化できる項数を表す。

【００３０】

【数３】

$$S_i = \alpha_i + m_{(i-1)H+1}\, b_1 b_2 \cdots b_{(i-1)H+1} + \cdots + m_{iH}\, b_1 b_2 \cdots b_{iH} \quad \cdots (9)$$

$$P^{(i)} < P^{(i-1)} < \cdots < P^{(0)} = P \quad \cdots (10)$$

【００３１】

下記（11）の関係が成立するので、順次、中間復号文M_I，M_{I-1}，・・・，M_2，M_1を算出することができ、メッセージ｛m_i｝を求めることができる。

【００３２】

【数４】

$$M_{i-1} \equiv \alpha_i^{-1} M_i \equiv \alpha_i^{-1} S_1 \cdot S_2 \cdot S_3 \cdots S_i \pmod{b_1 b_2 \cdots b_{(i-1)H+1}} \quad \cdots (11)$$

【００３３】

このような暗号系におけるメッセージ総長｜ｍ｜，暗号文長｜Ｃ｜及びレート（暗号化率）ｒは、近似的に夫々下記（12），（13）及び（14）で与えられる。

【００３４】

【数５】

$$|m| = HeI \quad \cdots (12)$$

$$|C| = (H+1)e\,\frac{I(I+1)}{2} \quad \cdots (13)$$

$$r = \frac{|m|}{|C|} = \frac{2H}{(H+1)(I+1)} \quad \cdots (14)$$

【００３５】

例えば、Ｉ＝２の場合、Ｈを十分大きくすると、レートｒは２／３に近づき、Ｉ＝３の場合には同様にレートｒは１／２に近づくことが分かる。

【００３６】

上記（８），（９）で表される中間復号文を展開して単純積和形式に変換した場合の項数Ｌは、$L=H(H+1)^{I-1}$ で与えられる。よって、本発明にて作成した暗号文に対してＬＬＬアルゴリズムによる攻撃を試みる場合には、$H(H+1)^{I-1}$ 次元のＬＬＬアルゴリズムを用いる必要があり、本発明による積和積形式の暗号文はＬＬＬアルゴリズムによる攻撃に強いことが分かる。

【００３７】

次に、他の復号処理について説明する。暗号文Ｃに対して、中間復号文M_I を下記（15）のようにして求める。

$$M_I \equiv T_1 \cdot T_2 \cdot T_3 \cdots T_I \pmod{P} \qquad \cdots (15)$$

但し、T_i は、下記（16）で表され、$P^{(i)}$ は、一般に下記（17）の条件を満たす大きな素数であり、Ｐのみを公開する。なお、下記（17）は、復号を補償した上で、$P^{(k)}$ が $P^{(k-1)}$ より小さいこと意味する。

【００３８】

【数６】

$$T_i = \alpha_i + \left(m_{(i-1)H+1} b_1^{(i,j)} + \cdots + m_{iH} b_1^{(i,j)} b_2^{(i,j)} \cdots b_H^{(i,j)} \right) B^{i-1} \qquad \cdots (16)$$

$$P^{(i)} \lesssim P^{(i-1)} \lesssim \cdots \lesssim P^{(0)} = P \qquad \cdots (17)$$

【００３９】

下記（18）の関係が成立するので、順次、中間復号文M_I，M_{I-1}，・・・，

M_2，M_1 を算出することができ、メッセージ｛m_i｝を求めることができる。

【００４０】

【数７】

$$M_{i-1} \equiv \alpha_i^{-1}\ T_1 \cdot T_2 \cdot T_3 \cdots T_i \quad (\mathrm{mod}\ B^{i-1})$$

・・・(18)

【００４１】

なお、上述した例では、積和積型の暗号文の場合について説明したが、上記（１）に示すように、複数の積和式を任意に組み合わせたそれらの乗算，加算結果により、暗号文Ｃを作成することが本発明において可能であることは勿論である。また、特願平10－262036号に提案した基数ベクトルとして$c_i = b_1\ b_2$ ・・・b_i を用いる方式に本発明を適用する場合について説明したが、特願平10－262037号に提案した基数ベクトルとして$c_i = d / d_i$ を用いる方式にも本発明を適用できる。更に、これらの各方式において乱数v_i を付加する場合にも、本発明は適用可能である。

【００４２】

図２は、本発明の記録媒体の実施の形態の構成を示す図である。ここに例示するプログラムは、平文ベクトルｍの一部と公開鍵ベクトルｃの一部とによる積和項を複数設定する処理と、設定したこれらの複数の積和項を積及び／または和の形式で結合して暗号文Ｃを作成する処理とを含んでおり、以下に説明する記録媒体に記録されている。なお、コンピュータ10は、各エンティティ側に設けられている。

【００４３】

図２において、コンピュータ10とオンライン接続する記録媒体11は、コンピュータ10の設置場所から隔たって設置される例えばWWW(World Wide Web)のサーバコンピュータを用いてなり、記録媒体11には前述の如きプログラム11a が記録されている。記録媒体11から読み出されたプログラム11a がコンピュータ10を制

御することにより、コンピュータ10が暗号文Ｃを作成する。

【００４４】

コンピュータ10の内部に設けられた記録媒体12は、内蔵設置される例えばハードディスクドライブまたはＲＯＭ等を用いてなり、記録媒体12には前述の如きプログラム12a が記録されている。記録媒体12から読み出されたプログラム12a がコンピュータ10を制御することにより、コンピュータ10が暗号文Ｃを作成する。

【００４５】

コンピュータ10に設けられたディスクドライブ10a に装填して使用される記録媒体13は、運搬可能な例えば光磁気ディスク，ＣＤ－ＲＯＭまたはフレキシブルディスク等を用いてなり、記録媒体13には前述の如きプログラム13a が記録されている。記録媒体13から読み出されたプログラム13a がコンピュータ10を制御することにより、コンピュータ10が暗号文Ｃを作成する。

【００４６】

【発明の効果】

以上詳述したように、本発明では、平文ベクトルの一部と公開鍵ベクトルの一部とによる複数の積和項を、更に、積及び／または和の形式で結合することによって暗号文を作成するようにしたので、ＬＬＬ法による攻撃に対して強くなり、安全性を向上することが可能となる。この結果、積和型暗号の実用化の道を開くことに、本発明は大いに寄与できる。

【００４７】

（付記）

なお、以上の説明に対して更に以下の項を開示する。

（１）　請求項１記載の暗号化方法であって、前記積和項の各項において前記平文をＫ分割した平文ベクトルの成分m_i （ｉ＝１，２，・・・，Ｋ）と$m_i\ c_i$ の形をとる前記公開鍵ベクトルの成分c_i を、整数b_i を用いて$c_i = b_1\ b_2 \cdots b_i$ に設定する暗号化方法。

（２）　請求項１記載の暗号化方法であって、前記積和項の各項において前記平文をＫ分割した平文ベクトルの成分m_i （ｉ＝１，２，・・・，Ｋ）と$m_i\ c_i$ の形をとる前記公開鍵ベクトルの成分c_i を、互いに素なＫ個の整数b_i を用い

てc_1＝d／d_1（但し、d＝d_1 d_2 ・・・d_K）に設定する暗号化方法。

（３）　複数のエンティティ間で暗号文による情報通信を行う暗号通信システムにおいて、請求項１，第（１），（２）項の何れかに記載の暗号化方法を用いて平文から暗号文を作成する暗号化器と、作成した暗号文を一方のエンティティから他方のエンティティへ送信する通信路と、送信された暗号文から元の平文を復号する復号器とを備える暗号通信システム。

（４）　コンピュータに、暗号化すべき平文を分割した平文ベクトルと公開鍵ベクトルとを用いて暗号文を作成させるためのプログラムが記録されているコンピュータでの読み取りが可能な記録媒体において、前記平文ベクトルの一部と前記公開鍵ベクトルの一部とによる積和項を複数設定することをコンピュータに実行させるプログラムコード手段と、設定した複数の積和項を積及び／または和の形式で結合することにより前記暗号文を作成することをコンピュータに実行させるプログラムコード手段とを含むプログラムが記録されている記録媒体。

【図面の簡単な説明】

【図１】

２人のエンティティ間における情報の通信状態を示す模式図である。

【図２】

記録媒体の実施の形態の構成を示す図である。

【符号の説明】

１　通信路

２　平文分割器

３　積和項設定器

４　暗号化器

５　復号器

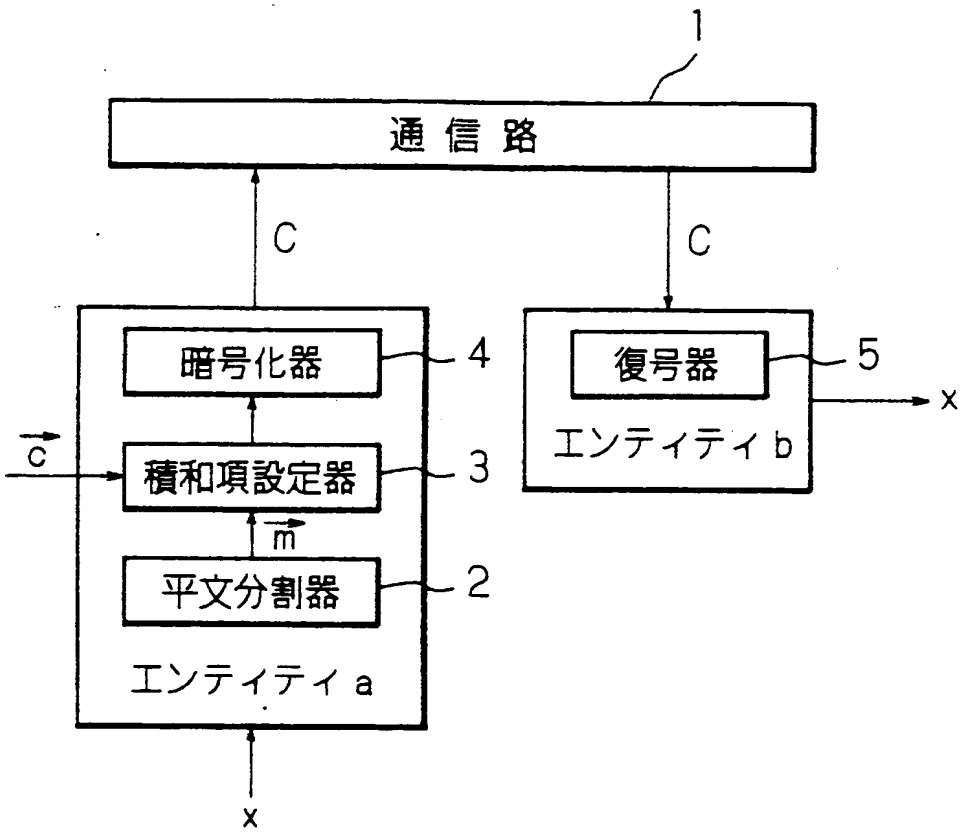
10　コンピュータ

11，12，13　記録媒体

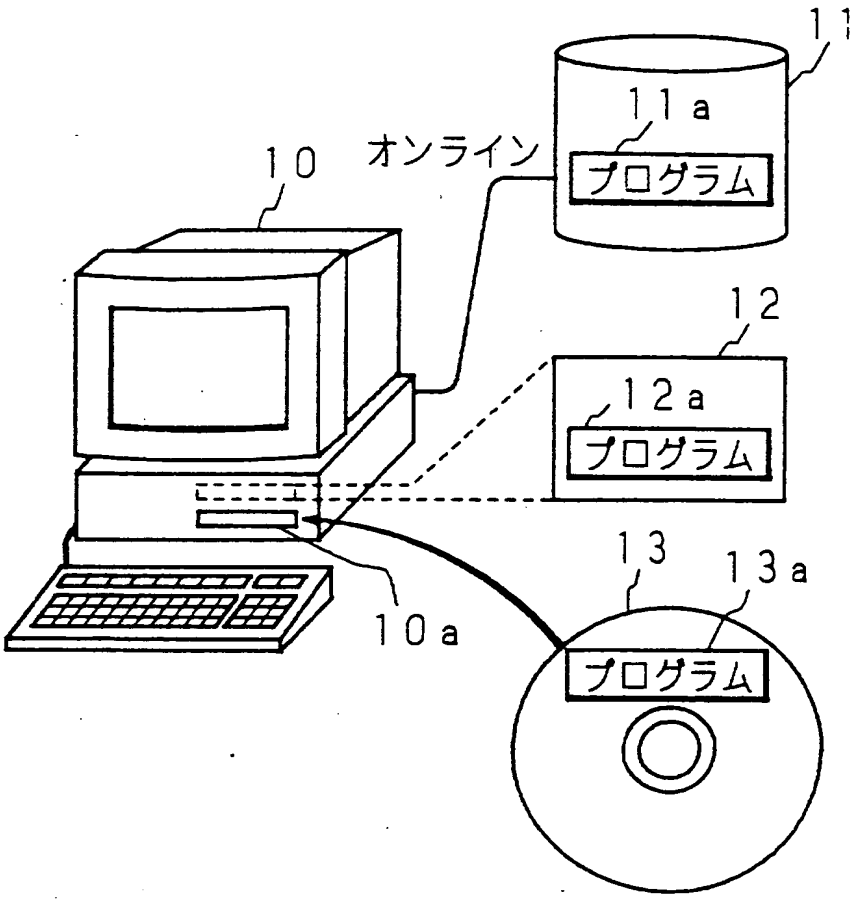
ａ，ｂ　エンティティ

【書類名】　　図面

【図１】



【図２】



【書類名】　　要約書

【要約】

【課題】　ＬＬＬ法による攻撃に対して強く、安全性を向上できる積和型暗号の暗号化方法を提供する。

【解決手段】　暗号化すべき平文を分割した平文ベクトルの一部と公開鍵ベクトルの一部とによる積和項を複数設定し、設定した複数の積和項を更に積及び／または和の形式で結合することにより暗号文を作成する。

【選択図】　　図１